Draft: 12/21/2006

December 15, 2006

Via Electronic Filing

Ms. Marlene Dortsch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re: Notice of Ex Parte Letter
In the Matter of Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities Video Relay Services; Misuse of Internet Protocol (IP) Relay Service and Video Relay Service

Dear. Ms. Dortsch,

The National Association of State Relay Administration (NASRA) wishes to commend the Federal Communications Commission for taking a proactive measure by requesting comments in an effort to seek a solution for controlling unlawful, fraudulent actions by persons using Internet Protocol (IP) relay services. NASRA would like to submit its comments and suggestions.

NASRA board members passed a motion in support of a registration procedure for IP relay services as a viable solution to reduce fraudulent relay calls and enhance E 9-1-1 relay calls. While several member states are on record as only supporting their state's comments, they have abstained from supporting the comments herein and will submit their own to the Commission. For the record, the comments that follow have the support of the majority of NASRA members.

In May 2006, the Commission requested comments from IP relay providers on methods they could use to control the prevalent and fraudulent use of IP relay services. Their comments indicated that they have taken action to block fraudulent relay calls, however, there is no evidence to support that any improvement has been made. Some providers claimed successful reduction in the abuse from 50% to 5% or less. This would imply that IP relay call volume would have also declined, but data from the last two years indicates that this is not so. This reinforces the opinion of NASRA members that the efforts of IP relay providers to reduce these fraudulent calls were rather unsuccessful. In addition, abuse of IP relay calls is not limited to fraudulent calls, but also includes obscene calls being placed by hearing persons (possibly teenagers). Reportedly, many businesses who have received fraudulent relay calls have resorted to blocking all relay calls, even legitimate ones from traditional TRS or video relay services.

In an effort to restrain the fraudulent abuse of IP relay services, some Internet providers have implemented the following procedures:

- Communications Assistants are given criteria that enable them to recognize a potentially fraudulent relay call, and when to alert the supervisor. The supervisor then may determine to warn the called party (business) of a possible scam, and may even suggest that the party terminate the call.

- IP addresses originating in a foreign country are blocked.
- Relay calls originating from the same IP addresses that indicate a pattern of fraudulent relay calls are identified, blocked and added to a database.

In the first procedure, the CA must render a subjective opinion while monitoring a call, and in so doing removes the transparency of the CA, – now no longer objective. The second procedure is flawed in that the determined scammer could easily register a domestic IP address, thus avoiding blockage of the foreign IP address. The third procedure disadvantages the unknowing visitor in another country when his/her legitimate call is blocked.

Some IP relay providers have noted that suspected fraudulent relay calls appear to be cyclical, with both high and low periods. IP relay providers estimated that periods of low attempts were the result of successful blockage, while high cycles meant scammers were anxious to find other IP addresses to which the systems were still vulnerable. Though security measures are being taken, fraud of this nature will continue to run rampant as long as there is large profit to be made.

It should be noted that when a CA identifies a fraudulent call and the IP relay provider alerts the called party or business, some choose to ignore it and proceed with the call. Whether or not the call is terminated, a call processed in any length is paid for by the TRS fund. Neither Congress nor the public would be in favor of subsidizing fraudulent relay calls, either in whole or in part.

The members of NASRA want to offer these suggestions to restrict fraudulent relay calls. Ideally, the members seek an objective solution that eliminates any subjective action by the CA, and one that is as functionally equivalent as possible. The members also recognize that the implementation of a registration procedure faces some strong resistance by consumers and some national organizations. There are those who claim that registration procedures would pose an undue burden on the users of IP relay without guaranteeing its effectiveness in controlling fraudulent relay calls. In addition, users are subject to greater inconvenience if they must register with each of the seven Internet Relay providers. These concerns are addressed, as well, with the following suggestions:

1) Registration Procedure: Internet Relay providers establish a one-time registration with a secure verification/authentication procedure for all IP Relay users. Registration also may include any information that the IP Relay user wishes to provide to expedite emergency IP relay calls.
2) Centralized registration database service: To ensure neutrality, the FCC secures a contract through a Request for Proposal for the services of a reputable, secure centralized registration/authentication database service. The service shall provide IP relay customers a user-friendly, secure and one-time registration procedure affording access to each IP relay provider

with only one log-on for all providers. The terms of the RFP will clearly define the requirements for a highly secure service and the penalties of any breach of confidentiality.

3) Verification procedure: Customers will be notified by U.S. mail of a confidential password or PIN, along with instructions for account activation. By calling a toll-free number, customers' identities are verified by ANI, and the account is activated. The IP relay customers now have access to **ANY** IP relay provider, as they now have the 'cookie' to access without the need to login each time at each site.

Should the FCC contract the services of a centralized registration database service as described, the abuse of IP relay calls to commit fraud would see an immediate decrease. While NASRA recognizes that this may not be the perfect solution, we acknowledge that this may begin to address the problems with IP Relay service almost immediately. Also, the members readily acknowledge that there may be technical issues with the above recommendations, and admittedly, there may be some viable solutions of which we may not yet be aware. It should be noted, however, that the relay providers do have resources to avail themselves of appropriate technical solutions for strong registration and verification/authentication procedures. It is possible that with enacting the proper rulings, incentives, and penalties, the IP relay providers may take the necessary action to resolve these issues.

User Friendly Biometric Fingerprint Service - Another possible solution, either now or in the near future, is a centralized registration database service that provides a biometric fingerprint database registration and verification processing service. One NASRA member recently had the opportunity to speak to a representative of a business that specializes in this technology. The company maintains a neutral database of all identified fingerprints,, provides a verification procedure service, and offers several levels of security protocols .The fingerprint reader device, about the size of a mouse and USB-based, takes only seconds to identify and authorize an identity, while the verification process takes about five to ten minutes.

This company, which has contracts with high-profile companies as well as government agencies, presumably has highly effective security protocols. Initially, the company verifies the registrants' identities, and then provides fingerprint readers to the customers, either through the mail or by the providers' service technicians. For scammers attempting to breach the system, they could potentially establish a United States mailing address and have a fingerprint reader forwarded to them out of country; however, obtaining their fingerprint on record would be a great deterrent. Theoretically, the fingerprint readers could be provided to IP relay users at no charge, with the cost passed on to the Interstate TRS fund. The use of this type of service could greatly minimize fraudulent relay calls.

In November, 2006, the FCC held an E 9-1-1 Summit that focused on accessibility for persons who are deaf, hard-of-hearing and speech-disabled. One of the topics addressed was the accessibility for users of Internet-based relay services to Public Safety Answering Points (PSAPs) when calling 9-1-1. NASRA members believe that whatever viable solutions evolve, they must also have a user-friendly registration/verification process for all IP relay providers in order to control the abuse of their services effectively.

In light of the lack of confidence on the part of businesses that use relay services, the members of NASRA recognize the importance and need of educational outreach efforts to counter this. These efforts must demonstrate that telecommunications relay services are viable and trustworthy, not only for persons who are deaf, deaf/blind, hard-of-hearing, or speech-disabled, but also for persons who do business with them. If the business entities have assurance from relay service providers that they are reputable, reliable and sound, then this will have positive effect on IP relay services. Regardless of the end solution, NASRA members strongly suggest that educational outreach be included. As a result, these efforts would also demonstrate to elected officials, such as Congress, the FCC's endeavors to resolve the problem.

Conclusion

NASRA takes a very strong position on the inappropriateness for any IP relay communications assistant (CA) to intervene in any relay call to monitor, block or terminate calls believed to be illegitimate based on criteria defined by the IP relay providers. To do so removes the objectivity of the communications assistant, a clearly unacceptable practice. Regardless of the legality of the criteria used to identify and track fraudulent calls, to notify call recipients or to terminate a call deemed illegitimate by IP relay service calls provider clearly violates the ADA's functional equivalency requirements.

With the rise in abuse of IP relay services, further delay in resolving the problem will result in even more damage to the quality and credibility of IP relay service in part and of all relay services including traditional relay services as a whole.

The NASRA members stress the importance of educational outreach, especially to business owners. However, outreach itself may be ineffective as any new legislation and its enforcement evolves. Time, energy and money will be needed to reinforce the outreach, while relay users still struggle to compete with the failing reputation of IP relay calls.

In closing, we hope the FCC will consider our suggestions to deal with the problem of fraudulent relay calls through Internet relay services. It is certainly a time-sensitive one, growing worse with time. It requires proactive measures to implement an enforceable solution in order to restore confidence in an established, trusted and critical service in the telecommunications industry.

Respectfully Submitted By:

Brenda Kelly-Frey, Chair of NASRA

cc: Board

NASRA Members